STIC Search Report
EIC 2100

STIC Database Tracking Number: 182718

TO: Cam-Linh T Nguyen **Location: RND 3C21** **Art Unit: 2161** **Tuesday, March 21, 2006** **Case Serial Number: 09/741680**	**From: Lucy Park** **Location: EIC 2100** **RND-4B11** **Phone: 571-272-8667** **lucy.park@uspto.gov**

Search Notes

Dear Examiner Nguyen,

Here are the search results for your Fast & Focused search request on case number 09/741680. Please let me know if you have any questions about these or if you need any further information.

Lucy

STIC EIC 2100 /82718
Search Request Form

Today's Date: 3/21/06

What date would you like to use to limit the search?
Priority Date: 12/15/00 Other:

Name Nguyen, Cam Linh
AU 2161 Examiner # 78921
Room # RND-3C21 Phone 24024
Serial # 09/741,680

Format for Search Results (Circle One):
PAPER DISK EMAIL

Where have you searched so far?
USP DWPI EPO JPO ACM IBM TDB
IEEE INSPEC SPI Other _____

Is this a "Fast & Focused" Search Request? (Circle One) (YES) NO
A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

- Administrative function with sensitive (infor. user)
- "Security officer" & normal administrator

STIC Searcher Lucy Park Phone 28667
Date picked up 3/21/06 Date Completed 3/21/06

STIC Search Results Feedback Form

EIC 2100

Questions about the scope or the results of the search? Contact ***the EIC searcher or contact:***

Anne Hendrickson, EIC 2100 Team Leader
272-3490, RND 4B28

Voluntary Results Feedback Form

- *I am an examiner in Workgroup:* ☐ *Example: 2133*
- *Relevant prior art **found**, search results used as follows:*
  - ☐ 102 rejection
  - ☐ 103 rejection
  - ☐ Cited as being of interest.
  - ☐ Helped examiner better understand the invention.
  - ☐ Helped examiner better understand the state of the art in their technology.

Types of relevant prior art found:

- ☐ Foreign Patent(s)
- ☐ Non-Patent Literature
  (journal articles, conference proceedings, new product announcements etc.)

- *Relevant prior art **not found:***
  - ☐ Results verified the lack of relevant prior art (helped determine patentability).
  - ☐ Results were not useful in determining patentability or understanding the invention.

Comments:

Drop off or send completed forms to STIC/EIC2100 RND, 4B28

altavista Web Images MP3/Audio Video News Family Filter: off Help

Advanced Web Search

Build a query with...

all of these words:	database role
this exact phrase:	multiple security levels
any of these words:	sensitive user
and none of these words	

SEARCH: ◉ Worldwide ○ USA **RESULTS IN:** ◉ All languages ○ English, Spanish

AltaVista found 17 results

High Assurance Multilevel Services For Off-The-Shelf Workstation Applications
File type:PDF - Download PDF Reader
... sharing of **sensitive** information by users at. **multiple security levels** ... obtained by several projects. including both **database** systems, e.g ... classes [10] or mandatory **role**-based policies ...
www.cs.nps.navy.mil/people/faculty/irvine/publications/older/MLS_LAN_nissc98.pdf
More pages from cs.nps.navy.mil

High Assurance Multilevel Services For Off-The-Shelf Workstation Applications
File type:PDF - Download PDF Reader
... sharing of **sensitive** information by users at. **multiple security levels** ... obtained by several projects. including both **database** systems, e.g ... classes [10] or mandatory **role**-based policies ...
csrc.nist.gov/nissc/1998/proceedings/paperF11.pdf
More pages from csrc.nist.gov

Protecting your network with firewalls, featuring Sun's SunScreen EFS firewall - SunWorld - January 1998
... are threatened. **Multiple security levels** will at ... system, data, and **user** levels. Security ... **database** server and the secure channel provides data privacy of proprietary or **sensitive** ...
sunsite.uakom.sk/sunworldonline/swol-01-1998/swol-01-efs.html
More pages from sunsite.uakom.sk

defense message system working group statehouse inn, montgomery al
... individual, or **role** (a global directory ... But **Sensitive** Messaging -- Classified Messaging CENTRAL COMPONENTS: - DMS **USER** AGENT ... 000 Terminals) - **Multiple Security Levels**: -- UNCLAS ...
www.mis.nps.navy.mil/~budden/xnplans/afplan/afdmsmtg
More pages from mis.nps.navy.mil

Proposal to Establish the Northern Virginia Metacomputing Center
... distances so that the **user** is unaware of physical ... Census Bureau's census and survey **database**. Often the amount ... Because of the central **role** of information-intensive applications ...
www.galaxy.gmu.edu/meta/metacomp.html

More pages from galaxy.gmu.edu

www2.cddc.vt.edu/www.eff.org/Activism/fed_email_policy_omb.report
Sally Katzen, Administrator, Office of Information and Regulatory Affairs (OIRA), of the Office of Management and Budget (OMB), chartered an interagency task force to address "Electronic Messaging Among Federal Agencies." ... **user** training programs in order to prevent, detect, and correct security problems. As with most information systems, internal threats, such as the misuse or release of **sensitive** ...
www2.cddc.vt.edu/www.eff.org/Activism/fed_email_policy_omb.report
More pages from www2.cddc.vt.edu

DARPA - 61 Phase I Selections from the 99.1 Solicitation
... can play a unique **role** in the design of multifunctional ... objects and objects stored in a **database**. Image Corp, Inc ... sensor enables a remote **user** to "look around" and assess ...
www.dodsbir.com/selections/abs991darpa.htm
More pages from dodsbir.com

packetstormsecurity.nl/docs/rainbow-books/NCSC-TR-002.txt
This approach can be used in conjunction with TDI developed systems or in the cases where the TDI does not apply. ... spirit of the "Trusted **Database** Management System Interpretation (TDI ... systems support highly **sensitive** and critical U.S. missions ... users must access **multiple security levels** in near ...
packetstormsecurity.nl/docs/rainbow-books/NCSC-TR-002.txt
More pages from packetstormsecurity.nl

Result Pages: 1 Back To Top

Advanced Web Search

H

◉ **Build a query with...**

all of these words:	database role
this exact phrase:	multiple security levels
any of these words:	sensitive user
and none of these words	

○ **Search with...**

this boolean expression

Use terms such as AND, OR, NOT
More>>

SEARCH: ◉ Worldwide ○ USA **RESULTS IN:** ◉ All languages ○ English, Spanish

Date: ○ by timeframe: Anytime

◉ by date range: 1 January 1980
15 December 2000

File type: Any format

Location

◉ by domain:

○ By URL:

Display:

☐ site collapse (on/off) What is this?

10 results per page

Clear Settings

Try your Search on Yahoo!

Business Services Submit a Site About AltaVista Privacy Policy Help

Sign in

Google

Web Images Groups News Froogle Local more »

database "multiple administrator" roles Search Advanced Search Preferences

Web Results **1** - **10** of about **310** for **database** "**multiple** **administrator**" **roles**. (**0.18** seconds)

[PDF] Microsoft PowerPoint - Lotusphere_2006_BES41_Preview.ppt
File Format: PDF/Adobe Acrobat - View as HTML
Support for **Multiple Administrator Roles**. • Group-based Administration. • Support for DB2 ... If **database** remotely installed, then insure that DB2 ...
www.blackberry.com/news/events/ pdfs/lotusphere_2006_bes41_preview.pdf - Similar pages

Secure Computing: Sidewinder G2 Enterprise Manager - Product overview
... Distributed hierarchical administrator **roles**; Record locking circumvents ... SQL **database** architecture; Simultaneous, **multiple administrator** access ...
www.securecomputing.com/index.cfm?sKey=1133&pf=1 - 12k - Cached - Similar pages

> Secure Computing: Sidewinder G2 Enterprise Manager - Product overview
> Highly flexible SQL **database** architecture; Simultaneous, **multiple administrator** access; Organize appliances to mirror your network; Create unlimited, ...
> www.securecomputing.com/index.cfm?sKey=1133 - 38k - Cached - Similar pages
> [More results from www.securecomputing.com]

Cisco CNS Network Registrar Users's Guide Web Interface, 6.0 ...
Global administrator—Responsible for the Central Configuration Manager (CCM) **database**. You should limit access to this **role**. host-admin ...
www.cisco.com/en/US/products/sw/netmgtsw/ ps1982/products_user_guide_chapter09186a0080154e53.html - 121k - Cached - Similar pages

> [PDF] Global Administration
> File Format: PDF/Adobe Acrobat - View as HTML
> administrative **roles** and access security, and monitors **database** changes and tasks. ... (Note, however, that you can also handle these **multiple administrator** ...
> www.cisco.com/univercd/cc/td/doc/ product/rtrmgmt/ciscoasu/nr/nr60/webui/03admin.pdf - Similar pages

Needs Assessment
Security & Administration, **Multiple administrator roles** with many levels of privilege ... Data encrypted inside **database**. Tests & Quizzes, Built-in quizzes, ...
caucuscare.com/inf_needs.shtml - 19k - Cached - Similar pages

[PPT] Notes and Domino 6.5.1 What's New and How It Will Help You Win ...
File Format: Microsoft Powerpoint - View as HTML
Programmability restrictions – control what applications can/can't do! **Database** signing and Execution Control Lists. **Multiple Administrator Roles** ...
www.sga.com/.../$FILE/ Are%20you%20getting%20the%20most%20from%20your%20Domino%20investment.ppt - Similar pages

ChrisBallam.com: Chris Ballam's Resume
Duties include Web design, **database** design and modeling, ... and **multiple Administrator** sections with different user administration **roles** and access ...
www.chrisballam.com/resume/index.htm - 29k - Cached - Similar pages

www.ORAsearch.com - Dedicated Career Site for Oracle professionals!
Also Monitoring the health and server efficiency and **DataBase** Performance tuning is something I would ... Worked daily with **multiple Administrator role** for ...
www.orasearch.com/ADIdocs5/ DetailOpen.cfm?detail_id=192820 - 21k -
Cached - Similar pages

ActivCard Secure Remote Access Solution (Two-factor 2005 ...
... delegation of **multiple administrator roles** if the situation calls for it. ... ActivCard provides an integrated **database** that controls both the tokens ...
www.scmagazine.com/.../4c60c7ba-7b6e-4f1d-ae03-bbcb94ddb3ae/ activcard-secure-remote-access-solution-/ - 39k - Cached - Similar pages

Try your search again on Google Book Search

Goooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

database "multiple administrator" rol Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

```
File 347:JAPIO Nov 1976-2005/Nov(Updated 060302)
        (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200619
        (c) 2006  Thomson Derwent

Set     Items   Description
S1     669919   USER? ? OR ACCOUNT? ? OR USERNAME? ?
S2      10847   S1(3N)(SENSITIV??? OR CLASSIFIED OR RESTRICT??? OR SECRET -
             OR SECRECY OR PRIVILEG??? OR PRIVATE OR PRIVACY OR SECUR???)
S3      32499   ADMINISTRATOR? ? OR OFFICER? ? OR ADMIN? ? OR SYSADMIN? ? -
             OR AUTHORITY OR AUTHORITIES
S4        146   S3(3N)(NORMAL OR REGULAR OR BASIC OR USUAL OR UNCLASSIFIED
             OR (NON OR "NOT")()(SENSITIVE OR CLASSIFIED OR RESTRICT??? OR
             SECRET OR PRIVILEG??? OR PRIVATE OR SECUR???))
S5        814   S3(3N)(SPECIAL OR SECUR??? OR TOP OR HIGH??? OR SENSITIV???
              OR CLASSIFIED OR RESTRICT??? OR SECRET OR SECRECY OR PRIVILE-
             G??? OR PRIVATE)
S6       8442   (S3 OR AUTHORIZ??? OR AUTHORIS??? OR AUTHORIZATION? ? OR A-
             UTHORISATION? ? OR SECURITY OR ACCESS)(3N)(LEVEL? ? OR TIER? ?
              OR ROLE? ? OR TYPE? ?)
S7          12   S2 AND (S4 OR S5) AND S6
S8           6   S7 NOT AD=20001215:20031215/PR
S9           5   S8 NOT AD=20031215:20060321/PR
S10          3   S4 AND S5
S11         74   S2 AND (S4 OR S5)
S12         62   S11 NOT (S7 OR S10)
S13         36   S12 NOT AD=20001215:20031215/PR
S14         30   S13 NOT AD=20031215:20060321/PR
S15     268717   DATABASE? ? OR DATABANK? ? OR DATASTORE? ? OR DB OR DBMS OR
              RDBMS OR RDB OR DATA()(BASE? ? OR BANK? ? OR STORE? ?)
S16          5   S15 AND S14
S17       1601   (S3 OR MANAGER? ?)(3N)(TWO OR THREE OR SECOND OR THIRD OR -
             NEXT OR ANOTHER OR ADDITIONAL OR MULTI OR MULTIPLE OR PLURAL?-
             ?? OR MANY OR SEVERAL OR NUMEROUS OR VARIOUS)
S18         97   S17 AND (S2 OR S4 OR S5 OR S6)
S19          9   S18 AND S15
S20          9   S19 NOT (S7 OR S10 OR S16)
S21         94   (S14 OR S18) AND IC=(G06F OR H04L)
S22         80   S21 NOT (S7 OR S10 OR S16 OR S20)
S23         61   S22 NOT AD=20001215:20031215/PR
S24         56   S23 NOT AD=20031215:20060321/PR
S25        368   S2 AND S6
S26         63   S25 AND S15
S27         58   S26 AND IC=(G06F OR H04L)
S28         29   S27 NOT AD=20001215:20031215/PR
S29         24   S28 NOT AD=20031215:20060321/PR
S30         23   S29 NOT (S7 OR S10 OR S16 OR S20)
S31         54   SECURITY()OFFICER? ?
S32          8   S31 AND S15
S33          7   S32 NOT (S7 OR S10 OR S16 OR S20 OR S30)
? logoff hold
       21mar06 10:44:58 User259273 Session D346.5
```

9/5/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013032013
WPI Acc No: 2000-203864/200018
XRPX Acc No: N00-151628
Flexible DCE user management design method through GSO provides concept of policy object giving flexibility in specifying attributes and granting admin users privileges for new functions
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
RD 429144	A	20000110	RD 99429144	A	19991220	200018	B

Priority Applications (No Type Date): RD 99429144 A 19991220
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
RD 429144	A		2	G06F-000/00	

Abstract (Basic): RD 429144 A
NOVELTY - Policy object defines values for some DCE user related attributes which GSO server will refer to in creating DCE user, also indicates if these DCE user management functions are allowed via GSO or not, and if yes what **levels** of **admin** users will have authority to perform new functions. The object currently contains 3 pairs of attributes and values and can be expanded for other policies in the future.
USE - For providing flexible DCE user management through GSO.
ADVANTAGE - Provides flexibility in specifying attributes and granting **admin users privileges** for the new functions, the concept of policy object is invented.
pp; 2 DwgNo 0/0
Title Terms: FLEXIBLE; USER; MANAGEMENT; DESIGN; METHOD; THROUGH; CONCEPT; OBJECT; FLEXIBLE; SPECIFIED; ATTRIBUTE; ADMINISTER; USER; NEW; FUNCTION
Derwent Class: T01
International Patent Class (Main): G06F-000/00
File Segment: EPI

9/5/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010305330
WPI Acc No: 1995-206590/199527
XRPX Acc No: N95-161895
Certifying public keys of digital signature in secure communications system - requiring user to present authority for verification key PKU to check if user **knows** secret **signing key associated with verification key**
Patent Assignee: MICALI S (MICA-I)
Inventor: MICALI S
Number of Countries: 002 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5420927	A	19950530	US 94189248	A	19940201	199527	B
WO 9521495	A1	19950810	WO 95US1327	A	19950201	199537	
AU 9517394	A	19950821	AU 9517394	A	19950201	199547	
US 5420927	B1	19970204	US 94189248	A	19940201	199711	

Priority Applications (No Type Date): US 94189248 A 19940201
Cited Patents: US 4326098; US 5214702; US 5261002; US 5299263; US 5307411
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5420927	A		6	H04K-001/00	
WO 9521495	A1	E	19	H04K-001/00	
AU 9517394	A			H04K-001/00	Based on patent WO 9521495
US 5420927	B1		3	H04K-001/00	

Abstract (Basic): US 5420927 A
The method for certifying pieces of data in a secure communications system with at least two **levels** of **authorities** , involves presenting a piece of data requiring certification to a first- **level authority** for inspection of a given property. If the piece of data passes the inspection of the first- **level** authority, the first- **level authority** sends to a **higher authority** a digital signature indicating that the piece of data has passed the inspection of the first- **level authority** .
If the digital signature of the first- **level authority** is correct, the **higher authority** issues a certificate, which does not include a signature of the first **level authority** , that the piece of data possesses the given property. The piece of data presented is a verification key of a digital signature scheme. The given property of the presented verification key is that a given user has chosen the verification key to be the public key.
ADVANTAGE - Facilitates widespread verification of digital signatures of users.
Dwg.0/0
Title Terms: CERTIFY; PUBLIC; KEY; DIGITAL; SIGNATURE; SECURE; COMMUNICATE; SYSTEM; REQUIRE; USER; PRESENT; AUTHORISE; VERIFICATION; KEY; CHECK; USER ; SECRET; SIGN; KEY; ASSOCIATE; VERIFICATION; KEY
Derwent Class: W01
International Patent Class (Main): H04K-001/00

International Patent Class (Additional): H04L-009/00
File Segment: EPI

10/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014796657 **Image available**
WPI Acc No: 2002-617363/200266
XRPX Acc No: N02-488562
Database system management method in distributed computing system, involves executing administrative function if object is not sensitive and function execution command is received from normal **database** administrator
Patent Assignee: SAMAR V (SAMA-I)
Inventor: SAMAR V
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020078049	A1	20020620	US 2000741680	A	20001215	200266	B

Priority Applications (No Type Date): US 2000741680 A 20001215
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020078049	A1		9	G06F-017/30	

Abstract (Basic): US 20020078049 A1
NOVELTY - A command is received to perform an administrative function involving an object defined within the database system. The administrative function is performed, if the object is not sensitive and if the command is received from a **normal** database **administrator** (134) for the system. The function is restricted from execution if the object is sensitive and command is received from **security officer** (136).
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:
(1) Computer readable storage medium storing database system management program; and
(2) Database system management apparatus.
USE - For managing database system storing sensitive, confidential data such as salary information, in distributed computing system.
ADVANTAGE - Provides the capability to store the sensitive data in encrypted form, while minimizing the number of database administrators needed to access the encrypted data, thereby reducing the security problem arising from allowing a large number of system administrators to have access to the encrypted data.
DESCRIPTION OF DRAWING(S) - The figure shows the schematic view of the distributed computing system.
Database administrator (134)
Security officer (136)
pp; 9 DwgNo 1/4
Title Terms: DATABASE; SYSTEM; MANAGEMENT; METHOD; DISTRIBUTE; COMPUTATION; SYSTEM; EXECUTE; ADMINISTER; FUNCTION; OBJECT; SENSITIVE; FUNCTION; EXECUTE; COMMAND; RECEIVE; NORMAL; DATABASE; ADMINISTER
Derwent Class: T01
International Patent Class (Main): G06F-017/30
International Patent Class (Additional): G06F-012/14; H04L-009/32
File Segment: EPI

your application

10/5/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013493341 **Image available**
WPI Acc No: 2000-665284/200064
XRPX Acc No: N00-493048

Cryptographic key distribution method for data communication, involves allocating private and public keys selected similar to selection of identity and sub- secret **for subordinate** administrators **to final operators**

Patent Assignee: TOTALFOERSVARETS FORSKNINGSINSTITUT (TOTA-N); FOERSVARETS FORSKNINGSANSTALT (FOER-N)
Inventor: BENGTSSON A
Number of Countries: 020 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200064098	A1	20001026	WO 2000SE721	A	20000414	200064	B
SE 9901358	A	20001017	SE 991358	A	19990416	200064	
SE 515778	C2	20011008	SE 991358	A	19990416	200161	

Priority Applications (No Type Date): SE 991358 A 19990416
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200064098	A1	E	21	H04L-009/32	
				Designated States (National): JP US	
				Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE	
SE 9901358	A			H04L-009/32	
SE 515778	C2			H04L-009/32	

Abstract (Basic): WO 200064098 A1

NOVELTY - **Basic secret** and subordinate **administrators** (A1-A3) are selected by a main administrator (A). Identity in the form of unique prime number is provided to all administrators and associated final operators. Sub-secret is allocated to subordinate **administrators** . **Private** and public keys selected similar to selection of identity and sub- **secret** for subordinate **administrators** , are allocated to final operators.

USE - For data communication in communication network.

ADVANTAGE - Implements automatic handling of chains of certificates in nodes of the type radiosets. Enables to form a common secret, replace change of certificates with identities in certification authority hierarchy and cause implicit certification of public keys.

DESCRIPTION OF DRAWING(S) - The figure shows the hierarchical structure of main and subordinate administrators.

Main administrator (A)
Subordinate administrators (A1-A3)
pp; 21 DwgNo 1/1

Title Terms: CRYPTOGRAPHIC; KEY; DISTRIBUTE; METHOD; DATA; COMMUNICATE; ALLOCATE; PRIVATE; PUBLIC; KEY; SELECT; SIMILAR; SELECT; IDENTIFY; SUB; SECRET; SUBORDINATE; FINAL; OPERATE
Derwent Class: W01
International Patent Class (Main): H04L-009/32
File Segment: EPI

20/5/5 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014708474 **Image available**
WPI Acc No: 2002-529178/200256
Related WPI Acc No: 2002-665836; 2003-017013
XRPX Acc No: N02-419089

Delegated administration of information in a database **directory uses arbitrary group of users, which enables an administrator to form administrative domains and sub-domains using the arbitrary group of users**

Patent Assignee: GENERAL ELECTRIC CO (GENE)
Inventor: AGGOUR K S; BARNETT J A; KORNFEIN M M; MEHRING D T; SEBASTIAN J; VIVIER B J
Number of Countries: 095 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200257881	A2	20020725	WO 2002US1336	A	20020116	200256 B
KR 2002084184	A	20021104	KR 2002711985	A	20020913	200320
US 20030163438	A1	20030828	US 2000241645	P	20001019	200357
			US 2001760995	A	20010116	
CN 1455905	A	20031112	CN 2002800100	A	20020116	200412
AU 2002239949	A1	20020730	AU 2002239949	A	20020116	200427
JP 2004525444	W	20040819	JP 2002558100	A	20020116	200455
			WO 2002US1336	A	20020116	
AU 2002239949	A8	20051013	AU 2002239949	A	20020116	200611

Priority Applications (No Type Date): US 2001760995 A 20010116; US 2000241645 P 20001019
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200257881	A2	E	45	G06F-000/00	
				Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW	
				Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW	
KR 2002084184	A			G06F-017/40	
US 20030163438	A1			G06F-007/00	Provisional application US 2000241645
CN 1455905	A			G06F-017/60	
AU 2002239949	A1			G06F-000/00	Based on patent WO 200257881
JP 2004525444	W		75	G06F-012/00	Based on patent WO 200257881
AU 2002239949	A8			G06F-017/60	Based on patent WO 200257881

Abstract (Basic): WO 200257881 A2

NOVELTY - Method for managing user information in a **database** directory, comprises: organizing the user information according to attribute values assigned to the information; specifying the organized user information into arbitrary group of users; and managing the user information associated with the arbitrary group of users.

DETAILED DESCRIPTION - INDEPENDENT CLAIM included for the following:method for providing delegated administration; user community administration tool; system; computer-readable medium

USE - For computer **databases** .

ADVANTAGE - Enables an administrator to form administrative domains and sub-domains using the arbitrary group of users. Also the delegated administrative tool enables an administrator to delegate administration and **various types** of administrative **authority** to other users within a community of users. Administration tool provides the

capability identify many different and arbitrary sets of users whose management is to delegated so that administration can be performed for any type of organization or community, regardless of its structure.

DESCRIPTION OF DRAWING(S) - The diagram shows an example of a user community.

pp; 45 DwgNo 1/10

Title Terms: ADMINISTER; INFORMATION; **DATABASE** ; DIRECTORY; ARBITRARY; GROUP; USER; ENABLE; ADMINISTER; FORM; ADMINISTER; DOMAIN; SUB; DOMAIN; ARBITRARY; GROUP; USER

Derwent Class: S05; T01

International Patent Class (Main): G06F-000/00; G06F-007/00; G06F-012/00; G06F-017/40; G06F-017/60

International Patent Class (Additional): G06F-012/14; G06F-015/16; G06F-017/30

File Segment: EPI

30/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

04571116 **Image available**
FILE SECURITY PROTECTION METHOD

PUB. NO.: 06-243016 [JP 6243016 A]
PUBLISHED: September 02, 1994 (19940902)
INVENTOR(s): ITO YUJI
APPLICANT(s): NIPPON DENKI COMPUTER SYST KK [000000] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 05-026387 [JP 9326387]
FILED: February 16, 1993 (19930216)
INTL CLASS: [5] **G06F-012/00** ; **G06F-012/14**
JAPIO CLASS: 45.2 (INFORMATION PROCESSING -- Memory Units)
JOURNAL: Section: P, Section No. 1835, Vol. 18, No. 630, Pg. 157, November 30, 1994 (19941130)

ABSTRACT

PURPOSE: To systematically and easily protect data on a file by adding a data class and a **security level** to the file attribute and prescribing the data class to which a user can access and the upper limit of the **security level** .

CONSTITUTION: When the user starts access to a system, a user management system 16 retrieves a user management **data base** 19 and reads an access right list obtained by combining the data class which the user can access and the upper limit of the **security level** into a memory. When the user requests the allocation of the file, a file management system 11 retrieves a file management **data base** 10, reads the data class and the **security level** of the file, recognizes that the data class is included in the access right list of the **user** and the **security level** does not exceed the upper limit of the **security level** of the **user** , and denies an allocation request when they violate the rules. Thus, a relation between data on the file and the user is arranged and systematic security which is easily managed is realized.

30/5/19 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009674689 **Image available**
WPI Acc No: 1993-368242/199346
XRPX Acc No: N93-284310
Determining direct and indirect access privileges **held by** database user **- displaying names of objects, identifying** type **of** access **to each object, and indicating whether such access privileges may be extended to others**
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: HOFFMAN R D
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5261102	A	19931109	US 91678572	A	19910328	199346	B

Priority Applications (No Type Date): US 91678572 A 19910328
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5261102	A		12	G06F-015/401	

Abstract (Basic): US 5261102 A

The method involves requesting a determination of objects to which a given **user** has access **privileges** . The objects to which the **user** has direct access **privileges** , and the objects to which the **user** has indirect access **privileges** are automatically determined. All access gps. to which the user belongs are automatically determined. The objects to which the access groups, determined above, have access privileges are automatically determined.

The **type** of **access** to each object to which the **user** has access **privileges** are automatically determined. It is determined whether the access privileges for each object to which the **user** has access **privileges** may be extended to others. The **access** privilege information, the **type** of **access** together with the respective object, and whether the access privileges may be extended to others, is provided to the user.

ADVANTAGE - ''Product independent'', can be imported to any **database** management program product. Implemented in non-procedural computer language.

Dwg.5/5

Title Terms: DETERMINE; DIRECT; INDIRECT; ACCESS; HELD; **DATABASE** ; USER; DISPLAY; NAME; OBJECT; IDENTIFY; TYPE; ACCESS; OBJECT; INDICATE; ACCESS; EXTEND
Derwent Class: T01
International Patent Class (Main): **G06F-015/401**
File Segment: EPI

```
File   2:INSPEC 1898-2006/Mar W2
         (c) 2006 Institution of Electrical Engineers
File   6:NTIS 1964-2006/Mar W1
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2006/Mar W2
         (c) 2006 Elsevier Eng.  Info. Inc.
File  23:CSA Technology Research Database 1963-2006/Mar
         (c) 2006 CSA.
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W2
         (c) 2006 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2006/Feb
         (c) 2006 ProQuest Info&Learning
File  65:Inside Conferences 1993-2006/Mar 20
         (c) 2006 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2006/Dec W4
         (c)2006 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Feb
         (c) 2006 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 13
         (c) 2006 The Gale Group
File 144:Pascal 1973-2006/Feb W4
         (c) 2006 INIST/CNRS
File 239:Mathsci 1940-2006/Apr
         (c) 2006 American Mathematical Society
File 256:TecInfoSource 82-2006/Feb
         (c) 2006 Info.Sources Inc

Set     Items   Description
S1    2313296   USER? ? OR ACCOUNT? ? OR USERNAME? ?
S2      17710   S1(3N)(SENSITIV??? OR CLASSIFIED OR RESTRICT??? OR SECRET -
             OR SECRECY OR PRIVILEG??? OR PRIVATE OR PRIVACY OR SECUR???)
S3     502465   ADMINISTRATOR? ? OR OFFICER? ? OR ADMIN? ? OR SYSADMIN? ? -
             OR AUTHORITY OR AUTHORITIES OR MANAGER? ?
S4       1220   S3(3N)(NORMAL OR REGULAR OR BASIC OR USUAL OR UNCLASSIFIED
             OR (NON OR "NOT")()(SENSITIVE OR CLASSIFIED OR RESTRICT??? OR
             SECRET OR PRIVILEG??? OR PRIVATE OR SECUR???))
S5      17918   S3(3N)(SPECIAL OR SECUR??? OR TOP OR HIGH??? OR SENSITIV???
              OR CLASSIFIED OR RESTRICT??? OR SECRET OR SECRECY OR PRIVILE-
             G??? OR PRIVATE)
S6      37380   (S3 OR AUTHORIZ??? OR AUTHORIS??? OR AUTHORIZATION? ? OR A-
             UTHORISATION? ? OR SECURITY OR ACCESS)(3N)(LEVEL? ? OR TIER? ?
              OR ROLE? ? OR TYPE? ?)
S7         44   S2 AND (S4 OR S5) AND S6
S8         38   RD  (unique items)
S9         31   S8 NOT PY=2001:2006
S10       100   S4 AND S5
S11        24   S10 AND (S2 OR S6)
S12        24   RD  (unique items)
S13        24   S12 NOT S9
S14        20   S13 NOT PY=2001:2006
S15   1108341   DATABASE? ? OR DATABANK? ? OR DATASTORE? ? OR DB OR DBMS OR
              RDBMS OR RDB OR DATA()(BASE? ? OR BANK? ? OR STORE? ?)
S16         2   S15 AND S10
S17       190   S15 AND S2 AND S6
S18     20333   S3(3N)(TWO OR THREE OR SECOND OR THIRD OR NEXT OR ANOTHER -
             OR ADDITIONAL OR MULTI OR MULTIPLE OR PLURAL??? OR MANY OR SE-
             VERAL OR NUMEROUS OR VARIOUS)
S19         0   S18 AND S17
S20      1094   S18 AND S15
S21        85   S20 AND (S2 OR S6)
S22        69   RD  (unique items)
```

```
S23          57   S22 NOT PY=2001:2006
S24          44   S23 NOT RD=20001215:20060321
S25          44   S24 NOT (SS9 OR S14 OR S16)
S26          44   S25 NOT PD=20001215:20060321
S27         717   SECURITY()OFFICER? ?
S28          27   S27 AND S2
S29          22   RD  (unique items)
S30          16   S29 NOT PY=2001:2006
S31          14   S30 NOT (S9 OR S14 OR S16)
? logoff hold
       21mar06 11:37:16 User259273 Session D346.10
```

9/5/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

07636374 INSPEC Abstract Number: C2000-08-6130S-026
Title: An adaptable security manager **for real-time transactions**
Author(s): Son, S.H.; Zimmerman, R.; Hansson, J.
Author Affiliation: Dept. of Comput. Sci., Virginia Univ., Charlottesville, VA, USA
Conference Title: Proceedings 12th Euromicro Conference on Real-Time Systems. Euromicro RTS 2000 p.63-70
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 2000 Country of Publication: USA xiii+281 pp.
ISBN: 0 7695 0734 4 Material Identity Number: XX-2000-01451
U.S. Copyright Clearance Center Code: 0 7695 0734 4/2000/$10.00
Conference Title: Proceedings 12th Euromicro Conference on Real-Time Systems. Euromicro RTS 2000
Conference Date: 19-21 June 2000 Conference Location: Stockholm, Sweden
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: The rising demand for real-time services over networks, such as Web-based information services, requires new approaches for balancing competing demands on limited resources. The BeeHive database system proposes a novel solution to this need by the use of adaptive real time, fault tolerance, quality of service and security services based on rules embedded in individual objects. These rules prescribe tradeoffs of alternate levels of service (and cost) when resource contention becomes a problem. The approach momentarily trades off the **level** of **security** to achieve the required real-time performance. In many situations, this is an acceptable, and even preferred, solution. We have developed an adaptable **security manager** to provide alternate levels of communications **security** to multiple **users** and to dynamically adapt to real-time performance conditions. In this paper, we present the design and evaluation of the proposed **security manager** that utilizes the notion of adaptable security services. (6 Refs)
Subfile: C
Descriptors: adaptive systems; distributed databases; fault tolerant computing; information resources; quality of service; real-time systems; security of data; telecommunication security; transaction processing
Identifiers: adaptable **security manager** ; real-time transactions; real-time network services; World Wide Web-based information services; competing demands; limited resources; BeeHive database system; adaptive real-time system; fault tolerance; service quality; adaptable security services; embedded rules; service levels; cost levels; resource contention; **security level** ; real-time performance; multi- **user** communications **security** ; real-time performance conditions; adaptable tradeoffs; multi-**level security**
Class Codes: C6130S (Data security); C6160B (Distributed databases)

9/5/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

07547297 INSPEC Abstract Number: B2000-05-6210C-011, C2000-05-5620-015
Title: Dynamic monitoring for security management based on state transition
Author(s): Heejin Jang; Sangwook Kim
Journal: Journal of KISS(A) (Computer Systems and Theory) vol.26, no.12 p.1468-75
Publisher: Korea Inf. Sci. Soc,
Publication Date: Dec. 1999 Country of Publication: South Korea
CODEN: CKNOF2 ISSN: 1226-2315
SICI: 1226-2315(199912)26:12L.1468:DMSM;1-M
Material Identity Number: E345-2000-004
Language: Korean Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: It is highly required to quickly detect the vulnerability of a computer network system and an appropriate action toward it should be followed as soon as possible for its security. It leads us to the need of a monitoring schema that can provide an integrated security management with carefully selected and analysed data through the computer network for its users. This paper presents a formal model of dynamic monitoring for security management. It provides the comprehensive security management using continuously changing **security** information, **user** interactions and dynamic activation of visual and monitoring objects. It enables system **security officers** to manage computer systems accurately, efficiently and conveniently by reflecting the state transition and the transformation of concerns and a monitoring **level** of system **security officers** immediately. This model can be used as the basis of a monitoring platform. (3 Refs)
Subfile: B C
Descriptors: computer network management; security of data
Identifiers: security management; state transition; integrated security management; monitoring schema; computer network; dynamic monitoring
Class Codes: B6210C (Network management); C5620 (Computer networks and techniques); C6130S (Data security); C0310D (Computer installation management)

9/5/3 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

07396782 INSPEC Abstract Number: C1999-12-6130S-031
Title: An integrity enforcement application design and operation framework in role **-based** access **control systems: A session-oriented approach**
Author(s): HyungHyo Lee; BongNam Noh
Author Affiliation: Dept. of Comput. Sci., Chonnam Nat. Univ., Kwangju, South Korea
Conference Title: Proceedings of the 1999 ICPP Workshops on Collaboration and Mobile Computing (CMC'99). Group Communications (IWGC). Internet '99 (IWI'99). Industrial Applications on Network Computing (INDAP). Multimedia Network Systems (MMNS). Security (IWSEC). Parallel Computing '99 (IWPC'99). Parallel Execution on Reconfigurable Hardware (PERH) p.179-84
Editor(s): Panda, D.; Takizawa, M.
Publisher: IEEE, Los Alamitos, CA, USA
Publication Date: 1999 Country of Publication: USA xxi+622 pp.
ISBN: 0 7695 0353 5 Material Identity Number: XX-1999-01656
U.S. Copyright Clearance Center Code: 0 7695 0353 5/99/$10.00
Conference Title: Proceedings of the 1999 ICPP Workshops
Conference Sponsor: Inf. Process. Soc. Japan (IPSJ); Int. Assoc. Comput. & Commun. (IACC); Univ. Aizu, Japan; Ohio State Univ., USA
Conference Date: 21-24 Sept. 1999 Conference Location: Aizu-Wakamatsu, Japan
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: **Role** -based **access** control (RBAC) policy is being widely accepted not only as an access control policy but as a flexible permission management framework in various commercial environments. RBAC simplifies the process of security management by assigning permissions to roles not directly to individual **users** . As **security administrators** can design and manage security policies by changing the configuration of RBAC components to meet their organization's own security needs, RBAC is called policy-neutral and has ability to articulate enterprise-specific security policies. While most researches on RBAC are for defining, describing model in formal method and other important properties such as separation of duty, little work has been done on how applications should be designed and then executed in automated information systems based on RBAC security model. In this paper, we describe important, dynamic features of a session that can be used as a vehicle for building applications, and present a basic framework for session-oriented integrity enforcement application design and operation applicable to commercial environments. (15 Refs)
Subfile: C
Descriptors: access protocols; security of data
Identifiers: integrity enforcement; access control; session-oriented approach; RBAC; access control policy; flexible permission management; security management; commercial environments
Class Codes: C6130S (Data security); C5640 (Protocols)

9/5/6 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

06282876 INSPEC Abstract Number: C9607-6130S-060
Title: Role **-based** access **control in real systems**
Author(s): Parker, T.; Sundt, C.
Journal: Information Systems Security vol.5, no.1 p.26-37
Publisher: Auerbach Publications,
Publication Date: Spring 1996 Country of Publication: USA
ISSN: 1065-898X
SICI: 1065-898X(199621)5:1L.26:RBAC;1-K
Material Identity Number: F173-96001
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: **Role** -based **access** control can be used to support the real-world access control requirements of a distributed system. This article describes a role model as used in the context of a distributed security infrastructure such as SESAME or OSF/DCE security. It is based on practical experience in the use of roles in real products and shows how **role** -based **access** control benefits both the **user** and the **security manager** . It also highlights the key practical issues that needed to be resolved in deriving this model. (7 Refs)
Subfile: C
Descriptors: authorisation; distributed processing; open systems
Identifiers: **role** -based **access** control; real-world access control; distributed system; role model; distributed security infrastructure; SESAME ; OSF/DCE; **security manager** ; user benefits
Class Codes: C6130S (Data security); C6150N (Distributed systems software)

9/5/7 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC

04181422 INSPEC Abstract Number: C88043164
Title: An EDP auditor's look at Top Secret
Author(s): Decker, A.
Journal: EDPACS vol.15, no.10 p.5-10
Publication Date: April 1988 Country of Publication: USA
CODEN: EDPCDF ISSN: 0736-6981
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P); Product Review (R)
Abstract: CA-TOP SECRET, if properly installed and implemented, it can provide comprehensive security for a variety of resources and MVS subsystems. The level of protection provided is directly related to the implementation and subsequent administration of the product. This article provides the auditor with the points that should be addressed during an audit of its implementation and administration. The author considers: ACIDs (accessor-IDs), modes of operation, ownership, **level** of **access** , Top **Secret** files, **user** attributes, reporting capabilities; administrative **authorities** for auditors; **security administrators** ; auditing the **security** database and other security concerns. (0 Refs)
Subfile: C
Descriptors: auditing; DP management; IBM computers; security of data
Identifiers: IBM MVS/370 environments; IBM MVS/XA environments; CA-TOP SECRET; ACIDs; accessor-IDs; modes of operation; ownership; **level** of **access** ; Top Secret files; user attributes; reporting capabilities; administrative authorities for auditors; **security administrators** ; security database
Class Codes: C0310D (Installation management); C6130 (Data handling techniques); C6150J (Operating systems)

9/5/8 (Item 8 from file: 2)
DIALOG(R)File 2:INSPEC

02644255 INSPEC Abstract Number: C81008901
Title: Grant levels **in an** authorization **mechanism**
Author(s): Paredaens, J.; Ponsaert, F.
Author Affiliation: Dept. of Math., Univ. Instelling Antwerpen, Wilrijk, Belgium
Journal: Information Processing Letters vol.11, no.4-5 p.152-5
Publication Date: 12 Dec. 1980 Country of Publication: Netherlands
CODEN: IFPLAT ISSN: 0020-0190
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: In some database systems the possibility exists to give grants, and if necessary to revoke them afterwards. The creator of some file or table is the only **user** who has the **privilege** to use that file or table, unless he grants the **privilege** to another **user** . The main purpose of an MIS is to provide information to management. In this framework the management has an hierarchical structure in which a level is associated to every manager. A **manager** can give **privileges** to its direct inferiors. Usually these privileges may be granted on and on only until a given maximal distance, down the hierarchy. A generalization is proposed: whenever a privilege is granted by a user, a level is associated indicating the maximum distance at which a privilege can be granted. (3 Refs)
Subfile: C
Descriptors: database management systems; management information systems; security of data
Identifiers: authorization mechanism; database systems; grants; hierarchical structure; MIS; management information systems; security of data
Class Codes: C6160 (Database management systems (DBMS)); C7100 (Business and administration)

9/5/10 (Item 2 from file: 6)
DIALOG(R)File 6:NTIS

1568356 NTIS Accession Number: AD-A230 437/6
Example Secure System Specified Using the Terry-Wiseman Approach
Harrold, C. L.
Royal Signals and Radar Establishment, Malvern (England).
Corp. Source Codes: 053783000; 409929
Sponsor: Defence Research Information Centre, Orpington (England).
Report No.: RSRE-90011; DRIC-BR-115326
Jul 90 65p
Languages: English
Journal Announcement: GRAI9112
Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A04/MF A01
Country of Publication: United Kingdom
This report presents the specification of operations for a secure document handling system (SERCUS). The specification uses the Terry-Wiseman Security Policy Model and therefore acts as an example of the modelling approach. The specification uses the mathematical notation Z, and consequently also acts as an example of the use of Z in specifying secure systems. However, it must be noted that an appreciation of SERCUS, the model and modelling approach can usefully be gained even if the formal specifications are not read. The Terry-Wiseman Model and its interpretation are given as an Annex to this report. SERCUS is essentially an electronic registry system which controls the creation of, and access to, classified documents and mail messages. In the usual way, the users are assigned clearances which limit their ability to observe and modify the information in the system. In addition to their clearance, the users have a designated role to play. The possible **roles** are **security officer** and ordinary **user** , although there were also registry clerks in the original, longer, specification. Certain operations may only be performed by users with the appropriate **role** . For example, only **security officers** may create new legal users or review journalled information and, in the original specification, only registry clerks could create files or add documents to files. Although the model does allow systems to be specified where individuals can have more than one role, this is not required in the SERCUS application, and each user is assigned a single fixed role.
Descriptors: *Documents; Classified materials; Electronic equipment; Files(Records); Handling; Law enforcement; Mathematics; Model theory; Officer personnel; Specifications
Identifiers: *Foreign technology; *Data processing security; NTISDODXA
Section Headings: 62GE (Computers, Control, and Information Theory--General)

01330764 ORDER NO: AADMM-81188

A DYNAMIC, EVENT-DEPENDENT DATA CONTROL: A USER-ROLE VIEW-BASED APPROACH

Author: MOHAMMED, IMTIAZ
Degree: M.A.SC.
Year: 1992
Corporate Source/Institution: UNIVERSITY OF WATERLOO (CANADA) (1141)
Source: VOLUME 32/01 of MASTERS ABSTRACTS.
PAGE 279. 158 PAGES
Descriptors: COMPUTER SCIENCE
Descriptor Codes: 0984
ISBN: 0-315-81188-9

Preventing the disclosure, modification or destruction of information held in a database is one of the most important considerations of a Database Management System and it has been the subject of active research for the past several years.

While Mandatory Access Control (MAC) assigns **security** clearance **levels** (e.g., top secret, secret) to all of the data to achieve access control, Discretionary Access Control (DAC) assigns **privileges** to **users** customized to their responsibilities within the application. The fundamental limitation with the above mechanisms is that they are unable to deal with the changing roles of a user (based on the occurrence of an event) within an application. As a result, **User - Role** Based **Security** (URBS) has been proposed as a means of addressing the above weaknesses.

In this thesis we demonstrate how URBS can be used to augment the existing security mechanisms. We first extend and enhance the URBS concept (originally proposed for the object-oriented model) to the relational model. The extension and enhancement include: (1) defining the notion of events in an application; and (2) requiring the Database **Administrator** to manage the **security** scheme. We then implement dynamic, event-dependent **user - role** based **security** in a prototype that runs on the Oracle DBMS. The prototype is tested and the results are evaluated. Finally, we draw conclusions and offer suggestions for further study.

26/5/11 (Item 11 from file: 2)
DIALOG(R)File 2:INSPEC

04602628 INSPEC Abstract Number: C90028391
Title: Analysis of the privacy model for the information system DORIS
Author(s): Biskup, J.; Graf, H.-W.
Author Affiliation: Inst. fur Inf., Hochschule Hildesheim, West Germany
Conference Title: Database Security, II. Status and Prospects. Results of the IFIP WG 11.3 Workshop p.123-40
Editor(s): Landwehr, C.E.
Publisher: North-Holland, Amsterdam, Netherlands
Publication Date: 1989 Country of Publication: Netherlands viii+281 pp.
ISBN: 0 444 87483 6
Conference Sponsor: Queens Univ
Conference Date: 5-7 Oct. 1988 Conference Location: Kingston, Ont., Canada
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: The information system DORIS has been designed to support privacy as the individual's right of informational self-determination. Technically it is based on careful adaptions of concepts for object oriented programming, relational **databases** and capability based operating systems. In the privacy model of DORIS there are **two** kinds of rights: **authorities** on **roles** (allowing operations) that are statically declared for groups (classes), and acquaintances (access capabilities) that are dynamically granted to specific persons (instances). Combined rights can also temporarily be made available. The dynamic distribution of rights within the system is analyzed by determining the largest set of acquaintances that a person can ever obtain. Known methods and results for capability based access control models are extended for treating the impact of the new concepts of authorities and availabilities. The analysis demonstrates that **database** administrators and privacy officers can reliably master the system. (10 Refs)
Subfile: C
Descriptors: data privacy; object-oriented programming; operating systems (computers); relational **databases** ; security of data
Identifiers: information system; DORIS; object oriented programming; relational **databases** ; capability based operating systems; privacy model; access control
Class Codes: C6160D (Relational DBMS); C6130 (Data handling techniques); C6150J (Operating systems)

31/5/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

04527566 INSPEC Abstract Number: C90008106
Title: VMS privilege masks-a method for controlling privileged tasks
Author(s): Goatley, H.
Author Affiliation: Clyde Digital Syst., Orem, UT, USA
Journal: VAX Professional vol.11, no.3 p.15-18
Publication Date: June 1989 Country of Publication: USA
CODEN: VAXPEN ISSN: 8750-9628
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: **Privileges** for each **account** on a VMS system are usually determined by the system manager or **security officer** for a site. The author discusses how such privileges are dispensed and their use to control access to privileged functions. (0 Refs)
Subfile: C
Descriptors: DEC computers; operating systems (computers); security of data
Identifiers: privileged task control; VMS system security; VAX system security; privilege masks; VMS system; system manager; **security officer**; privileges; privileged functions
Class Codes: C6150J (Operating systems); C6130 (Data handling techniques)